

Linear Precoding for Broadcast Channels with Confidential Messages under Transmit-Side Channel Correlation

Giovanni Geraci^{1,2}, Azzam Y. Al-nahari^{3,4}, Jinhong Yuan¹ and Iain B. Collings²

¹School of Electrical Engineering & Telecommunications, The University of New South Wales, AUSTRALIA

²Wireless and Networking Technologies Laboratory, CSIRO ICT Centre, Sydney, AUSTRALIA

³Department of Electrical and Information Technology, Lund University, SWEDEN

⁴Department of Electronics Engineering, Ibb University, YEMEN

Abstract

In this paper, we analyze the performance of regularized channel inversion (RCI) precoding in multiple-input single-output (MISO) broadcast channels with confidential messages under transmit-side channel correlation. We derive a deterministic equivalent for the achievable per-user secrecy rate which is almost surely exact as the number of transmit antennas and the number of users grow to infinity in a fixed ratio, and we determine the optimal regularization parameter that maximizes the secrecy rate. Furthermore, we obtain deterministic equivalents for the secrecy rates achievable by: (i) zero forcing precoding and (ii) single user beamforming. The accuracy of our analysis is validated by simulations of finite-size systems.

Index Terms

Physical layer security, channel correlation, broadcast channel, random matrix theory, linear precoding.

I. INTRODUCTION

Wireless multiuser communications are very susceptible to eavesdropping, and the transmitted information has traditionally been secured at the network layer with cryptographic schemes. However, this raises issues like key distribution and management, and high computational complexity. Moreover, these schemes rely on the unproven assumption that certain mathematical functions are hard to invert. Therefore, it is of critical importance to tackle security at the physical layer.

Physical layer security was introduced in [1], [2] to exploit the randomness inherent in noisy channels. The secrecy capacity region of a broadcast channel with confidential messages (BCC), where the intended users can act maliciously as eavesdroppers, was studied in [3], [4] among others, but only for the case of two users. For a larger BCC with any number of malicious users, it was shown in [5], [6] that regularized channel inversion (RCI) precoding can achieve large secrecy sum-rates with low-complexity implementation, if the channels are independent and identically distributed (i.i.d). However in practice, channel correlation is present due to local scatterers around the base station and insufficient separation between antennas. The large-system performance of RCI precoding in the broadcast channel (BC) without secrecy requirements under channel correlation was analyzed in [7], [8], where deterministic approximations were obtained for the sum-rates.

In this paper, we analyze the secrecy sum-rate achievable by RCI precoding in the multiple-input single-output (MISO) BCC under transmit-side channel correlation. This work directly extends some of the analysis in [7], [8] by requiring the transmitted messages to be kept confidential. Furthermore, this work generalizes the results in [5], [6], where no channel correlation was assumed. In the analysis, we provide a deterministic approximation for the large-system secrecy rates achievable by RCI precoding under transmit-side correlation, and we derive the optimal regularization parameter of the RCI precoder that maximizes the large-system secrecy rates. Then we obtain deterministic equivalents for the secrecy rates achievable by: (i) zero forcing precoding and (ii) single user beamforming. Simulations demonstrate that the analysis is accurate even when applied to finite-size systems.

II. MISO BCC UNDER TRANSMIT-SIDE CHANNEL CORRELATION

A. System Model

We consider the downlink of a narrowband multi-user MISO system, consisting of a base station (BS) with M antennas which simultaneously transmits K independent confidential messages to K spatially dispersed single-antenna users. In this model, transmission takes place over a block fading channel, and the transmitted signal is $\mathbf{x} = [x_1, \dots, x_M]^T \in \mathbb{C}^{M \times 1}$. The received signal at user k is given by

$$y_k = \sum_{j=1}^M h_{k,j} x_j + n_k \quad (1)$$

where $h_{k,j}$ is the channel between the j -th transmit antenna element and the k -th user, and n_k is the noise seen at the k -th receiver. The corresponding vector equation is

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \quad (2)$$

where $\mathbf{H} \in \mathbb{C}^{K \times M}$ is the channel matrix with entries $h_{k,j}$, $\mathbf{y} = [y_1, \dots, y_K]^T \in \mathbb{C}^{K \times 1}$ and $\mathbf{n} = [n_1, \dots, n_K]^T \in \mathbb{C}^{K \times 1}$. We assume that $\mathbb{E}[\mathbf{n}\mathbf{n}^\dagger] = \sigma^2 \mathbf{I}$, define the SNR $\rho \triangleq 1/\sigma^2$, and impose the long-term power constraint $\mathbb{E}[\|\mathbf{x}\|^2] = 1$. The transmitted signal \mathbf{x} is obtained at the BS by performing a linear processing on the vector of confidential messages $\mathbf{u} = [u_1, \dots, u_K]^T \in \mathbb{C}^{K \times 1}$, whose entries are chosen independently, satisfying $\mathbb{E}[|u_k|^2] = 1$. We assume homogeneous users, i.e. each user experiences the same received signal power on average, thus the model assumes that their distances from the transmitter are similar.

We consider correlation amongst transmit antenna elements, and for tractability in the analysis, we assume a separable (or Kronecker) correlation model [8], [9]. Hence the channel matrix can be written as

$$\mathbf{H} = \tilde{\mathbf{H}} \mathbf{R}^{\frac{1}{2}} \quad (3)$$

where $\tilde{\mathbf{H}} \in \mathbb{C}^{K \times M}$ contains i.i.d. circularly-symmetric complex Gaussian random variables, with zero mean and unit variance, and where $\mathbf{R} \in \mathbb{C}^{M \times M}$ is the non-singular transmit correlation matrix, given by $\mathbf{R} = \mathbb{E}[\mathbf{H}^\dagger \mathbf{H}]$. We assume that each user experiences the same transmit correlation. The channel vector for the k -th user is $\mathbf{h}_k^\dagger = \tilde{\mathbf{h}}_k^\dagger \mathbf{R}^{\frac{1}{2}} \in \mathbb{C}^{M \times 1}$.

It is required that the BS securely transmits each message u_k , ensuring that the unintended users receive no information. We assume that for each message u_k the $K - 1$ unintended users can cooperate to jointly eavesdrop on the intended user k , and form an equivalent single eavesdropper with $K - 1$ receive antennas, denoted by \tilde{k} . Although this is impossible in practice, such worst-case assumption is required to guarantee the secrecy of all messages, since the behavior of the users cannot be predicted. The secrecy sum-rate is given by

$$R_s \triangleq \sum_{k=1}^K R_k, \quad (4)$$

where each secrecy rate R_k is defined as the rate at which the BS communicates reliably to user k without allowing \tilde{k} to obtain any information about u_k .

B. Secrecy Sum-Rates with RCI Precoding

In RCI precoding, the transmitted vector is obtained as $\mathbf{x} = \mathbf{W}\mathbf{u}$, with the precoding matrix $\mathbf{W} \in \mathbb{C}^{M \times K}$ given by [10]

$$\mathbf{W} = [\mathbf{w}_1, \dots, \mathbf{w}_K] = \frac{1}{\sqrt{\gamma}} \mathbf{H}^\dagger (\mathbf{H}\mathbf{H}^\dagger + \xi M \mathbf{I}_K)^{-1} \mathbf{u}, \quad (5)$$

and

$$\gamma = \text{Tr}\{\mathbf{H}^\dagger \mathbf{H} (\mathbf{H}^\dagger \mathbf{H} + \xi M \mathbf{I}_M)^{-2}\} \quad (6)$$

is a long-term power normalization constant. The function of the real regularization parameter $\xi \geq 0$ is to achieve a tradeoff between the signal power at the intended user and the interference and information leakage at the unintended users for each message.

For the multi-user MISO system with malicious users, a secrecy sum-rate R_s achievable by linear precoding was found in [5] by considering that each user k , along with its own eavesdropper \tilde{k} and the transmitter, forms an equivalent multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel [11]. The transmitter, the intended receiver and the eavesdropper of each MISOME wiretap channel are equipped with M , 1 and $K - 1$ virtual antennas, respectively. Due to the simultaneous transmission of the K messages, the receiver k experiences noise and interference from all the messages u_j with $j \neq k$. Since the malicious users can cooperate, interference cancellation can be performed at

the receiver \tilde{k} , which does not see any undesired signal term apart from the received noise, and R_s represents a lower-bound on the achievable secrecy sum-rate.

For a given channel \mathbf{H} , let $\mathbf{H}_{\tilde{k}}$ be the matrix obtained from \mathbf{H} by eliminating the k -th row. Then a lower-bound on the secrecy sum-rate achievable by RCI precoding is [5]

$$R_s = \sum_{k=1}^K R_k = \sum_{k=1}^K \left\{ \log_2 \frac{1 + \frac{\rho |\mathbf{h}_k^\dagger \mathbf{w}_k|^2}{\gamma + \rho \sum_{j \neq k} |\mathbf{h}_k^\dagger \mathbf{w}_j|^2}}{1 + \frac{\rho}{\gamma} \|\mathbf{H}_{\tilde{k}} \mathbf{w}_k\|^2} \right\}^+. \quad (7)$$

In the following, we refer to (7) as the secrecy sum-rate.

III. LARGE SYSTEM ANALYSIS

In this section, we analyze the performance of the RCI precoder under transmit-side channel correlation in the large-system regime, where both the number of receivers K and the number of transmit antennas M approach infinity, with their ratio $\beta = K/M$ being held constant and finite.

A. Large-System Secrecy Sum-Rates

The following theorem provides a deterministic equivalent for the per-user secrecy rates R_k , which is almost surely exact as $M \rightarrow \infty$.

Theorem 1: Let $\rho > 0$, $\beta > 0$, and $\xi > 0$. Then for all k

$$|R_k - R^\circ| \xrightarrow{\text{a.s.}} 0, \quad \text{as } M \rightarrow \infty. \quad (8)$$

R° is the large-system secrecy rate, given by

$$R^\circ = \left\{ \log_2 \frac{1 + \eta \frac{\rho E_{22} + \frac{\xi \rho}{\beta} (1+\eta)^2 E_{12}}{\rho E_{22} + (1+\eta)^2 E_{12}}}{1 + \frac{\rho E_{22}}{(1+\eta)^2 E_{12}}} \right\}^+, \quad (9)$$

where

$$\eta = \mathbb{E} \left[\frac{\mathbf{T}(1+\eta)}{\xi(1+\eta) + \beta \mathbf{T}} \right], \quad \text{and} \quad E_{ij} = \mathbb{E} \left[\frac{\mathbf{T}^i}{(\xi(1+\eta) + \beta \mathbf{T})^j} \right]. \quad (10)$$

The expectations in (10) are taken over the random variable \mathbf{T} , whose distribution function $\Lambda(t)$ is the limiting eigenvalue distribution of the correlation matrix \mathbf{R} .

Proof: See Appendix A for a sketch of the proof. ■

We note that (9) is a non-random function of ρ , β , and ξ .

Corollary 1: In the case of no channel correlation, R° reduces to the value obtained in [6], given by

$$\tilde{R}^\circ = \left\{ \log_2 \frac{1 + g(\beta, \xi) \frac{\rho + \frac{\rho\xi}{\beta} [1 + g(\beta, \xi)]^2}{\rho + [1 + g(\beta, \xi)]^2}}{1 + \frac{\rho}{[1 + g(\beta, \xi)]^2}} \right\}^+, \quad (11)$$

where $g(\beta, \xi) \triangleq \frac{1}{2} \left[\sqrt{\frac{(1-\beta)^2}{\xi^2} + \frac{2(1+\beta)}{\xi}} + 1 + \frac{1-\beta}{\xi} - 1 \right]$.

Proof: See Appendix B for a sketch of the proof. ■

B. Selection of the Optimal Regularization Parameter

The value of ξ affects the asymptotic secrecy rate R° in (9). We now study the optimal regularization parameter $\xi^{\circ*}$ that maximizes R° under transmit-side channel correlation.

Theorem 2: The regularization parameter $\xi^{\circ*}$ that maximizes the secrecy rate R° under transmit-side channel correlation can be obtained by solving the fixed-point equation

$$\xi = \beta \frac{(\eta^2 - 1)E_{12} - \rho E_{22}}{2\rho\eta(1 + \eta)E_{12}}. \quad (12)$$

Proof: See Appendix C for a sketch of the proof. ■

We note that η , E_{12} , and E_{22} in (12) depend on ξ . It is easy to verify that the value of the regularization parameter $\xi^{\circ*}$ that maximizes R° differs from the value β/ρ that maximizes the rates without secrecy requirements [8]. Moreover in the presence of secrecy requirements, the channel correlation affects the optimal regularization parameter.

C. Comparison with Other Precoding Schemes

1) *Zero Forcing:* As the regularization parameter $\xi \rightarrow 0$, we have the zero forcing (ZF) precoder. The aim of the ZF precoder is to cancel all the interference and information leakage. With ZF precoding the transmitted signal is

$$\mathbf{x} = \begin{cases} \frac{1}{\sqrt{\gamma_0}} \mathbf{H}^\dagger (\mathbf{H}\mathbf{H}^\dagger)^{-1} \mathbf{u} & \text{for } \beta \leq 1 \\ \frac{1}{\sqrt{\gamma_0}} (\mathbf{H}^\dagger \mathbf{H})^{-1} \mathbf{H}^\dagger \mathbf{u} & \text{for } \beta > 1 \end{cases} \quad (13)$$

where γ_0 is the power normalization constant. It can be shown that in the large-system regime, the secrecy rates R_0° achievable by ZF precoding under transmit-side channel correlation are given by

$$R_0^\circ = \begin{cases} \log_2 \left(1 + \frac{\rho}{\chi} \right) & \text{for } \beta \leq 1 \\ \left\{ \log_2 \frac{1 + \frac{\rho}{\rho(\beta-1) + \beta^2 \gamma_0^\circ}}{1 + \frac{\rho(\beta-1)}{\gamma_0^\circ \beta^2}} \right\}^+ & \text{for } \beta > 1 \end{cases} \quad (14)$$

with

$$\chi = \frac{\beta}{\int \frac{td\Lambda(t)}{1+\chi t}} \quad \text{and} \quad \gamma_0^\circ = \frac{\beta-1}{\int \frac{d\Lambda(t)}{t}}. \quad (15)$$

2) *Single User Beamforming*: As the regularization parameter $\xi \rightarrow \infty$, we have the single user beamformer (SUB). Here, the transmitter beamforms in a direction such as to maximize the signal strength of each user, without taking into account the interference it creates and the amount of resulting information leakage. The SUB is given by

$$\mathbf{x} = \frac{1}{\sqrt{\gamma_\infty}} \mathbf{H}^\dagger \mathbf{u}, \quad (16)$$

where γ_∞ is the power normalization constant. It can be shown that the secrecy rates R_∞° achievable by SUB in the large-system regime and under transmit-side channel correlation are

$$R_\infty^\circ = \left\{ \log_2 \frac{1 + \frac{\rho \mathbb{E}^2[\mathbf{T}]}{\beta(\rho \mathbb{E}[\mathbf{T}^2] + \mathbb{E}[\mathbf{T}])}}{1 + \frac{\rho \mathbb{E}[\mathbf{T}^2]}{\mathbb{E}[\mathbf{T}]}} \right\}^+. \quad (17)$$

We note that when $\beta \geq 1$, it is $R_\infty^\circ = 0 \ \forall \rho$. When $\beta < 1$, there is always a value of ρ beyond which $R_\infty^\circ = 0$. Such poor performance is due to the intended user suffering from a large amount of interference, while the eavesdroppers may cancel the interference by cooperating.

IV. NUMERICAL RESULTS

Calculating R° in (9) requires the limiting eigenvalue distribution of the correlation matrix \mathbf{R} . In this section, we consider the Toeplitz-exponential model [12], where \mathbf{R} has a Toeplitz structure and its entries follow the distribution $r_{ij} = \nu^{|i-j|}$, governed by the correlation coefficient $\nu \in [0, 1]$. It can be shown that under Toeplitz-exponential correlation, the large-system secrecy rates R° reduce to

$$R_{TE}^\circ = \left\{ \log_2 \frac{1 + \eta \frac{\rho c + \frac{\xi \rho}{\beta} (1+\eta)^2}{\rho c + (1+\eta)^2}}{1 + \frac{\rho c}{(1+\eta)^2}} \right\}^+, \quad (18)$$

with $c = \frac{\xi(1+\eta)(1+\nu^2)+\beta(1-\nu^2)}{\xi(1+\eta)(1-\nu^2)+\beta(1+\nu^2)}$.

Fig. 1 compares the per-antenna secrecy sum-rate approximation $K R^\circ/M$ under transmit-side correlation to the simulated ergodic per-antenna secrecy sum-rate R_s/M with a finite number of users, for $\nu = 0.5$ and three values of β . The values of R° and R_s were obtained by (9) and (7), respectively, using $\xi = \xi^{\circ*}$ obtained as a positive solution to (12). We note that the accuracy of the analysis decreases with ρ . The loss of accuracy is due to the limitations of the tools used to derive the deterministic equivalents [7]. One can increase the accuracy at any given $\rho < \infty$ by increasing the dimension M .

Fig. 2 shows the relative secrecy rate loss $(\tilde{R}^\circ - R^\circ)/\tilde{R}^\circ$ due to channel correlation, with R° and \tilde{R}° from (9) and (11), respectively. We observe how low-to-moderate correlation, i.e. $\nu < 0.4$, does not affect the secrecy sum-rate excessively, i.e. the loss is less than 10 percent. However, higher correlation can significantly degrade the performance of the RCI precoder, especially at low SNR.

Fig. 3 shows that using the large-system regularization parameter $\xi^{\circ*}$ from (12) does not cause a significant loss in the secrecy sum-rate compared to using a finite-system regularization parameter $\xi = \xi^*$ optimized by bi-sectional search for each channel realization. The complementary cumulative distribution function (CCDF) of the normalized secrecy sum-rate difference $(R_s(\xi^*) - R_s(\xi^{\circ*}))/R_s(\xi^*)$ between using $\xi^{\circ*}$ and ξ^* depends on the values of SNR and β , where large SNR and $\beta = 1$ represent the worst case. The CCDFs in Fig. 3 were obtained for $\beta = 1$, and $\nu = 0.5$. Since the average normalized secrecy sum-rate difference is two percent or less for all values of M , the large-system regularization parameter $\xi^{\circ*}$ from (12) may be used instead of the finite-system regularization parameter with only a small loss of performance. Such choice avoids the computation of ξ^* for each channel realization.

V. CONCLUSION

In this paper, we considered regularized channel inversion (RCI) precoding for the MISO broadcast channel with confidential messages, under transmit-side channel correlation. We first analyzed the RCI precoder in the large-system regime, and derived a deterministic equivalent for the achievable per-user secrecy rate, as well as the optimal regularization parameter that maximizes the deterministic equivalent of the per-user secrecy rate. Then we obtained deterministic equivalents for the secrecy rates achievable

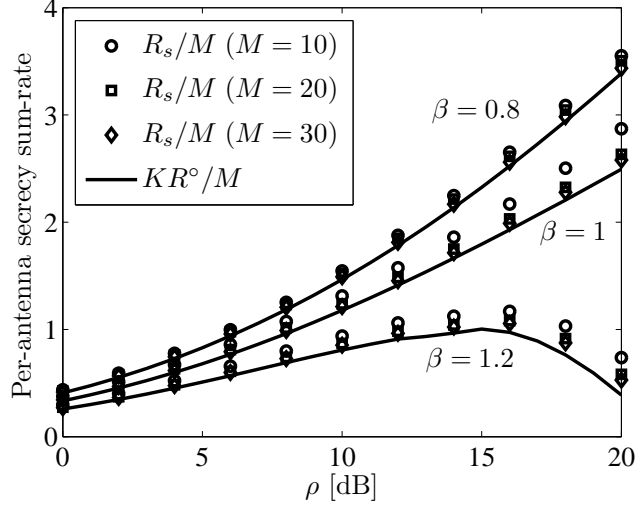


Fig. 1. Comparison between the simulated ergodic per-antenna secrecy sum-rate R_s/M from (7) and the large-system approximation KR°/M from (9), for $\nu = 0.5$ and various values of β .

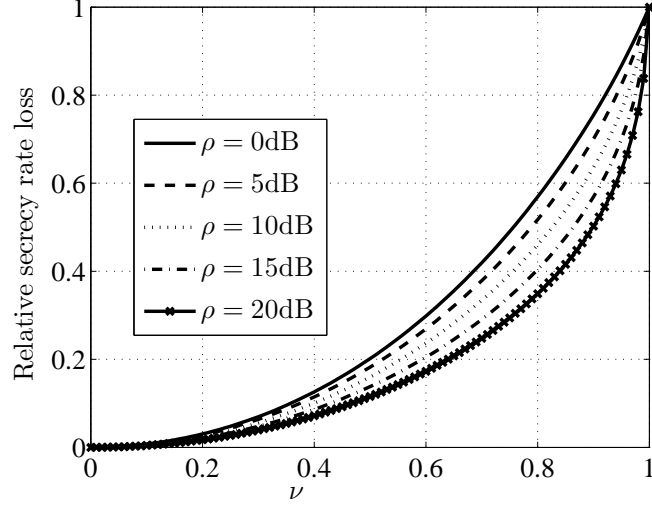


Fig. 2. Relative secrecy rate loss $(\tilde{R}^\circ - R^\circ)/\tilde{R}^\circ$ as a function of the correlation coefficient ν , for $\beta = 0.8$.

by: (i) zero forcing precoding and (ii) single user beamforming. The large-system approximations prove to be accurate even for finite-size systems. Simulations showed that low-to-moderate correlation only partially affects the secrecy rates. However, high correlation degrades the performance of the RCI precoder, especially at low SNR.

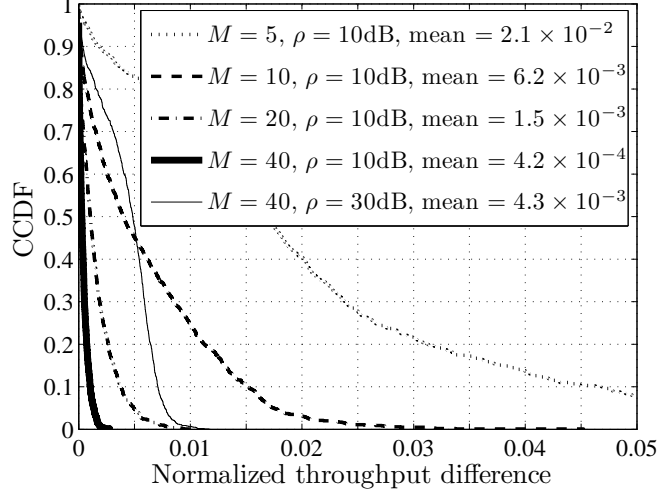


Fig. 3. CCDF of the normalized secrecy sum-rate difference between using: (i) $\xi^{\circ*}$ obtained from (12) and (ii) ξ^* obtained by bi-sectional search for every channel realization, for $\beta = 1$, and $\nu = 0.5$.

APPENDIX

A. Sketch of Proof of Theorem 1

By introducing the quantities [13]

$$A_k = \tilde{\mathbf{h}}_k^\dagger \mathbf{Q}_k \tilde{\mathbf{h}}_k, \quad B_k = \tilde{\mathbf{h}}_k^\dagger \mathbf{Q}_k \tilde{\mathbf{H}}_k^\dagger \tilde{\mathbf{H}}_k \mathbf{Q}_k \tilde{\mathbf{h}}_k, \quad \text{and} \quad \gamma = \text{Tr} \left\{ \mathbf{Q}_k \tilde{\mathbf{H}} \mathbf{R}^{-1} \tilde{\mathbf{H}}^\dagger \mathbf{Q}_k \right\}, \quad (19)$$

with $\mathbf{Q}_k = \left(\tilde{\mathbf{H}}_k^\dagger \tilde{\mathbf{H}}_k + M \xi \mathbf{R}^{-1} \right)^{-1}$, it is possible to express the secrecy rates as

$$R_k = \left\{ \log_2 \frac{1 + \frac{\rho A_k^2}{\rho B_k + \gamma(1+A_k)^2}}{1 + \frac{\rho B_k}{\gamma(1+A_k)^2}} \right\}^+. \quad (20)$$

As $M, K \rightarrow \infty$, the quantities in (19) respectively converge almost surely to [8]

$$A_k^\circ = \eta, \quad B_k^\circ = \frac{\beta E_{22}}{1 - \beta E_{22}}, \quad \text{and} \quad \gamma^\circ = -\frac{\beta}{(1 + \eta)^2} \frac{\partial \eta}{\partial \xi}, \quad (21)$$

where $\frac{\partial \eta}{\partial \xi} = \frac{-(1+\eta)^2 E_{12}}{1 - \beta E_{22}}$ and η , E_{12} and E_{22} are defined in (10). Then (9) follows from (20), (21), by applying the continuous mapping theorem, the Markov inequality, and the Borel-Cantelli lemma [14].

B. Sketch of Proof of Corollary 1

When no channel correlation is present, we have $\mathbf{R} = \mathbf{I}$ and $\Lambda(t) = \delta(t - 1)$, which implies $\eta = g$ and $E_{12} = E_{22} = [\xi(1 + g) + \beta]^{-2}$. Therefore $A_k^\circ = g$, $B_k^\circ = \frac{\beta g}{\xi(1+g)^2 + \beta}$, and $\gamma^\circ = \frac{\beta g}{\xi(1+g)^2 + \beta}$, and (11) follows.

C. Sketch of Proof of Theorem 2

We obtain eq. (12) by defining $\chi = (1 + \eta)^2 E_{12}$, $Z = (\beta E_{22} + \xi \chi)(\rho E_{22} + \chi)$, $\Psi = \frac{\beta E_{22} + \xi(1 + \eta)^2 E_{12}}{\rho E_{22} + (1 + \eta)^2 E_{12}}$, $\Phi = \frac{\rho^2 \Psi \eta \Lambda}{\beta Z}$, and $\Lambda = \frac{2\eta'(1 + \eta)E_{12}E_{22} + (1 + \eta)^2(E'_{12}E_{22} - E'_{22}E_{12})}{\eta'}$ [8], with $E'_{12}E_{22} - E'_{22}E_{12} = -2\beta(1 + \eta + \xi\eta')(E_{13}E_{33} - E_{23}^2)$, and solving

$$\frac{\partial R^\circ}{\partial \xi} = \frac{\eta'}{2^{R_s^\circ} \rho \chi^2 \beta (1 + \frac{\rho E_{22}}{\chi})^2 \log 2} [\Phi(\rho\xi - \beta)(\chi^2 + \rho\chi E_{22})\beta + \rho^2 \Lambda(\beta + \rho\eta\Psi)] = 0. \quad (22)$$

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, pp. 1355–1387, 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [3] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.
- [4] R. Liu, T. Liu, V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. PP, no. 99, 2013.
- [5] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.
- [6] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Sel. Areas Commun.*, 2013, accepted for publication. Available: arXiv:1304.5850.
- [7] S. Wagner, R. Couillet, M. Debbah, and D. T. M. Slock, "Large system analysis of linear precoding in correlated MISO broadcast channels under limited feedback," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4509–4537, July 2012.
- [8] R. Muharar and J. Evans, "Downlink beamforming with transmit-side channel correlation: A large system analysis," *Technical Report*, 2009, available: <http://www.cubinlab.ee.unimelb.edu.au/~rmuharar/doc/techRepCorr.pdf>.
- [9] T. Al-Naffouri, M. Sharif, and B. Hassibi, "How much does transmit correlation affect the sum-rate scaling of MIMO Gaussian broadcast channels?" *IEEE Trans. Commun.*, vol. 57, no. 2, pp. 562–572, 2009.
- [10] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication - Part I: Channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.
- [11] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
- [12] R. M. Gray, "Toeplitz and circulant matrices: A review," *Foundations and Trends in Commun. and Inf. Theory*, vol. 2, no. 3, 2005.
- [13] V. Nguyen and J. Evans, "Multiuser transmit beamforming via regularized channel inversion: A large system analysis," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2008, pp. 1–4.
- [14] R. Couillet and M. Debbah, *Random Matrix Theory Methods for Wireless Communications*. Cambridge University Press, 2011.